Amendments to the Claims:

This listing of claims replaces is provided for convenience. No amendments have been made.

Listing of Claims:

1. (Previously presented): A method for securing an accessible computer system, the method comprising:

monitoring for connection transactions between multiple access requestors and access providers using a switching component connected to the access providers, wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and

denying access by an attacking access requestor to the access providers when a number of connection transactions initiated by the attacking access requestor through the switching component exceeds a configurable threshold number during a first configurable period of time.

2. (Canceled)

3. (Previously Presented): The method as in claim 1, wherein the monitoring further includes counting, using the switching component, the number of connection transactions initiated by the access requestors to any of the access providers through the switching component during the first configurable period of time.

4. (Previously Presented): The method as in claim 3, wherein:

the monitoring further includes comparing, using the switching component, the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number, and

denying access by the attacking access requestor to the access providers includes denying, using the switching component, access by the attacking access requestor to all of the access providers connected to the switching component when the comparison results indicate that the number of connection transactions initiated by the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

5. (Canceled)

6. (Previously Presented): The method as in claim 1, wherein the monitoring further includes counting, using the switching component, the number of connection transactions initiated to any of the access providers by the Internet protocol addresses during the first configurable period of time such that the number of connection transactions reflects a cumulative number of connection transactions initiated to any of the access providers by the Internet protocol addresses.

7. (Previously Presented): The method as in claim 6, wherein the monitoring further includes comparing, using the switching component, the number of connection transactions initiated by the Internet protocol addresses during the first configurable period of time to the configurable threshold number, and

denying access by the attacking access requestor to the access providers includes denying, using the switching component, access by the attacking access requestor to all of the access providers connected to the switching component when the comparison results indicate that the number of connection transactions initiated by the Internet protocol address associated with the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

8. (Original): The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

9. (Previously presented): The method as in claim 1, wherein the detecting includes identifying the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

10. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

11. (Previously presented): The method as in claim 10, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

12. (Previously presented): The method as in claim 1, wherein the denying of access includes denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the attacking access requestor through the switching component.

13. (Previously presented): The method as in claim 1, wherein the access requestors are clients and the access providers are hosts such that the monitoring includes detecting connection transactions through the switching component between multiple clients and multiple hosts.

14. (Previously Presented): The method as in claim 3, wherein the counting further comprises counting, using the switching component, a cumulative number of connection transactions for all of the access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

15. (Previously presented): A system for securing an accessible computer system, comprising:

a switching component connected to access providers having means for:

monitoring for connection transactions between multiple access requestors and the access providers, wherein the monitoring includes detecting connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and

denying access by an attacking access requestor to the access providers when a number of connection transactions initiated by the attacking access requestor exceeds a configurable threshold number during a first configurable period of time.

16. (Previously Presented): The system of claim 15, wherein the switching component includes:

means for detecting connection transactions initiated by the access requestors through the switching component;

means for counting the number of connection transactions initiated by the access requestors to any of the access providers through the switching component during the first configurable period of time;

means for comparing the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number; and

the means for denying access by the attacking access requestor to the access providers includes means for denying access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions initiated by the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

17. (Previously Presented): The system of claim 15, wherein the switching component includes:

means for detecting connection transactions between the multiple Internet protocol addresses and the access providers using the switching component;

means for counting the number of connection transactions to any of the access providers initiated by the Internet protocol addresses through the switching component during the first configurable period of time such that the number of connection transactions reflects a cumulative number of connection transactions initiated to any of the access providers by the Internet protocol addresses;

means for comparing the number of connection transactions initiated by the Internet protocol addresses through the switching component during the first configurable period of time to the configurable threshold number; and

the means for denying access by the attacking access requestor to the access providers includes means for denying access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions initiated by the Internet protocol address associated with the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

18. (Original): The system of claim 17, wherein the means for monitoring includes means for monitoring a computer system for connection transactions made using TCP.

19. (Previously presented): The system of claim 17, wherein the means for detecting includes:

means for identifying the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

20. (Previously presented): The system of claim 15, wherein the switching component includes:

means for denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

21. (Previously presented): The system of claim 20, wherein the means for denying access further includes:

means for resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

22. (Previously presented): The system of claim 15, wherein the means for the switching component includes:

means for denying access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

23. (Previously presented): The system of claim 15, wherein the access requestors are clients and the access providers are hosts such that the means for the switching component includes:

means for detecting connection transactions through the switching component between multiple clients and multiple hosts.

24. (Previously Presented): The system of claim 16, wherein the means for counting further comprises means for counting a cumulative number of connection transactions for all of the access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

25. (Previously presented): A system for securing an accessible computer system, comprising:

a switching component connected to access providers to:

monitor for connection transactions between multiple access requestors and access providers, wherein to monitor for connection transactions include to detect connection transactions between multiple Internet protocol addresses and the access providers with the switching component; and

deny access by the access requestor to the access providers when a number of connection transactions initiated by an attacking access requestor exceed a configurable threshold number during a first configurable period of time.

26. (Previously Presented): The system of claim 25, wherein the switching component comprises:

a detection component that is structured and arranged to detect connection transactions initiated by the access requestors through the switching component;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access requestors to any of the access providers through the switching component during the first configurable period of time;

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access requestors through the switching component during the first configurable period of time to the configurable threshold number; and

the switching component is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions initiated by the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

27. (Previously Presented): The system of claim 25, wherein the switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between the multiple Internet protocol addresses and the access providers;

a counting component that is structured and arranged to count the number of connection transactions to any of the access providers initiated through the switching component by the Internet protocol addresses during the first configurable period of time such that the number of connection transactions reflects a cumulative number of connection transactions initiated to any of the access providers by the Internet protocol addresses;

a comparing component that is structured and arranged to compare the number of connection transactions initiated through the switching component by the Internet protocol addresses during the first configurable period of time to the configurable threshold number; and

the switching component is configured to deny access by the attacking access requestor to all of the access providers when the comparison results indicate that the number of connection transactions initiated by the Internet protocol address associated with the attacking access requestor during the first configurable period of time exceeds the configurable threshold number.

28. (Original): The system of claim 27, wherein the connection transactions include connections made using TCP.

29. (Previously presented): The system of claim 27, wherein the detection component comprises:

an identifying component that is structured and arranged to identify the Internet protocol addresses through the use of a header attached to a message representing the connection transaction being detected.

30. (Previously presented): The system of claim 25, wherein the switching component comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switching component by the attacking access requestor for a second configurable period of time.

31. (Previously presented): The system of claim 30, wherein the switching component further comprises:

a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access providers by the attacking access requestor.

32. (Previously presented): The system of claim 31, wherein the switching component further comprises:

a reset component that is structured and arranged to reset the timing component after detecting a new connection transaction initiated by the attacking access requestor through the switching component during the second configurable period of time.

33. (Previously presented): The system of claim 25, wherein the switching component comprises:

an access preventer that is structured and arranged to deny access to the access providers through the switching component by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

34. (Previously presented): The system of claim 25, wherein the access requestors are clients and the access providers are hosts such that the switching component comprises:

a detection component that is structured and arranged to detect connection transactions through the switching component between multiple clients and multiple hosts.

35. (Previously Presented): The system of claim 26, wherein the counting component further comprises counting a cumulative number of connection transactions for all of the access providers connected to the switching component initiated by each of the access requestors during the first configurable period of time.

36. (Previously presented): The system of claim 25, wherein a host computer system receives communications from the switching component.

37. (Previously presented): The system of claim 25, wherein the switching component is included in a host computer system.

38. (Previously Presented): The method of claim 1 wherein denying access by the attacking access requestor to the access providers when the number of connection transactions initiated by the attacking access requestor through the switching component exceeds a configurable threshold number during the first configurable period of time comprises denying, using the switching component, access by the attacking access requestor to all of the access providers connected to the switching component irrespective of which of the access providers to which the attacking access requestor initiated connection transactions to exceed the configurable threshold.

39. (Previously Presented): The method of claim 1 wherein the monitoring includes monitoring, using a switching component configured to establish communication links between access requestors and access providers, for attempts, by the attacking access requestor, to establish a communication link with any of the access providers.

40. (Previously Presented): The method of claim 39 wherein monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers includes monitoring for attempts, by the attacking access requestor, to establish a communication link with any of the access providers, the establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages.

41. (Previously Presented): The method of claim 11 further comprising:

determining, using the switching component, that the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component; and

in response to determining that the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component, allowing access by an attacking access requestor to the access providers.

42. (Previously Presented): The method of claim 1 wherein:

the access providers include a first access provider and a second access provider that is different from the first access provider;

monitoring for connection transactions between multiple access requestors and access providers using the switching component connected to the access providers includes:

detecting, using the switching component, a first number of connection transactions initiated by the attacking access requestor to the first access provider during the first configurable period of time, and detecting, using the switching component, a second number of connection transactions initiated by the attacking access requestor to the second access provider during the first configurable period of time, and

denying access by the attacking access requestor to the access providers when the number of connection transactions initiated by the attacking access requestor through the switching component exceeds the configurable threshold number during the first configurable period of time includes denying access by the attacking access requestor to both the first access provider and the second access provider when a sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number.

43. (Previously Presented): The method of claim 42 wherein:

detecting, using the switching component, the first number of connection transactions initiated by the attacking access requestor to the first access provider during the first configurable period of time includes detecting a first number of connection transactions that exceeds the configurable threshold number during the first configurable period of time,

detecting, using the switching component, a second number of connection transactions initiated by the attacking access requestor to the second access provider during the first configurable period of time includes detecting zero connection transactions initiated by the attacking access requestor to the second access provider during the first configurable period of time, and

denying access by the attacking access requestor to both the first access provider and the second access provider when a sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number includes denying access by the attacking access requestor to both the first access provider and the second access provider when the first number of connection transactions exceeds the configurable threshold number and the second number of connection transactions is zero.

44. (Previously Presented) The method of claim 42 wherein:

detecting, using the switching component, the first number of connection transactions initiated by the attacking access requestor to the first access provider during the first configurable period of time includes detecting a first number of connection transactions that is less than the configurable threshold number during the first configurable period of time,

detecting, using the switching component, a second number of connection transactions initiated by the attacking access requestor to the second access provider during the first configurable period of time includes detecting a second number of connection transactions that is less than the configurable threshold number during the first configurable period of time, the sum of the first number of connection transactions and the second number of connection transactions exceeding the configurable threshold number, and.

denying access by the attacking access requestor to both the first access provider and the second access provider when a sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number includes denying access by the attacking access requestor to both the first access provider and the second access provider when the sum of the first number of connection transactions and the second number of connection transactions exceeds the configurable threshold number, even though neither the first number of connection transactions nor the second number of connection transactions exceeds the configurable threshold number.

45. (Previously Presented) The method of claim 1 wherein:

the access providers include a first access provider and a second access provider that is different from the first access provider, and

the monitoring takes into account interactions of the attacking access requestor with both the first access provider and second access provider.